REMARKS

Claims 1-3 were rejected under 35 U.S.C. §102(b) as being anticipated by Holloway et al. (US 5,805,801). The applicant respectfully traverses this rejection for the following reason(s).

Note that in order for an anticipation rejection to be proper, the anticipating reference must disclose exactly what is claimed. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Note here that the Examiner has not relied on "inherency," accordingly, each and every element must be expressly described in Holloway.

Claim 1 calls for reading a MAC destination address and a MAC source address included in the received packet data; detecting, in an address table, access vectors corresponding to the MAC destination and source addresses; and denying access if the access vectors of the MAC destination and source addresses are not matched.

Holloway discloses the use of an authorized address list (AAL) controls which MAC addresses are allowed to connect to specified ports. **Each entry in the AAL consists of two fields: port number and authorized address**. The port number identifies a specific port on the hub; the authorized address field specifies the address or addresses that are allowed to connect to the port.

The AAL (**Authorized Address** List) defines which MAC addresses, *i.e.*, **authorized**

address, are allowed to connect to specific ports on the hub.

Claim 14 in Holloway is more specific in that is sets forth Holloway's invention as follows: "for each port, a source address of a station attempting to connect to said port with the authorized address list of addresses for said port and determining whether said source address is on said authorized address list."

Accordingly, Holloway discloses reading only a MAC source address included in the received packet data. Holloway fails to disclose *reading a MAC destination address and a MAC source address included in the received packet data* as required by claim 1.

"There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ2d 1001, 18 USPQ2d 1896 (Fed. Cir. 1991).

In this regard, the Examiner refers us to Holloway's Fig. 10, item 145 and Fig. 11, item 131.

Holloway's FIG. 10 depicts the processing that occurs in the interconnect devices during each iteration of the discovery phase*. This task responds to the receipt of a discovery request frame by sending a discovery response frame. In step 145 a source MAC address and time stamp are extracted for building the response. There is no destination MAC address being extracted.

Holloway's Fig. 11 depicts the processing that occurs in the managed hub in response to the receipt of a discovery response frame. This task maintains the state of this iteration of the discovery phase. In step 131 interconnect device information is extracted from the frame.

In step 132, an Interconnect Device List is searched for an item with a MAC address matching the **source address** of the discovery response frame.

There is no disclosure that the interconnect device information extracted in step 131 is based on a **destination MAC address**.

Holloway discloses that the Interconnect Device List is a list of the interconnect devices that responded in a previous discovery phase.

Holloway discloses that a discovery phase is initiated by each managed hub in the campus network. **Its purpose is to determine the LAN interconnect devices in the campus LAN that support the LAN security feature.**

*Each managed hub periodically transmits a discovery frame (FIG. 5A) to the LAN security feature group address. The managed hub then uses the information in the response frame (FIG. 5B) to build and maintain a list of all of the devices that support the LAN security feature. This list is referred to as the Interconnect Device List (ICD). The addresses in this list are used in the hub enable phase to correlate the reception of the filter set frame (FIG. 5D) with entries in the list. The managed hubs typically store these ICD lists in management information base (MIB) tables where they can be retrieved, upon request, from a network management station.

The discovery phase can also be used to provide an integrity check on the ICD list of devices supporting the LAN security feature. By periodically transmitting the discovery frame (FIG. 5A) to the LAN security feature group address, checks can then be made to ensure that all of the devices are still in the ICD security list. If any discrepancies are detected, e.g., if a station is removed from the list or added to the list, then an SNMP trap is sent to the network management station. This

notification alerts the network administrator that a potential security exposure exists in the campus network. FIG. 6 illustrates the structure of the ICD list along with the information stored in the list for each discovered interconnect device.

Accordingly, Figs. 10 and 11 in Holloway are directed towards discovering what devices are connected to a managed hub in order to create an Interconnect Device List (ICD) which identifies those devices authorized to be connected to the hub.

There is no disclosure in Holloway equating the MAC source and destination addresses **of received packet data received** *upon request of communication through at least one port of a plurality of ports of an Ethernet switch* with the Interconnect Device information gathered upon interconnect device discovery phase.

The Examiner has taken excerpts of Holloway's disclosure out of context in an attempt to reject the Applicant's claims.

Accordingly, the rejection is deemed to be in error and should be withdrawn.

Additionally, Holloway clearly discloses checking an authorized address list (AAL table) of a port for source MAC addresses to determine whether the source MAC address is on the authorized address list. If the source MAC address is on the list, then the source desiring to communicate through the port is authorized and allowed to use that port.

Accordingly, there is no address table comprised of access vectors corresponding to both the

MAC destination and source addresses. In fact there is no address table comprised of access vectors disclosed in Holloway at all.

Instead, the Examiner appears to equate Holloway's AAL table with the Applicant's address table of access vectors.

Consider a MAC address of, for example, 00:00:f0:aa:bb:cc. In Holloway the source address is compared to source addresses in the AAL table. In the present invention, both the source address and the destination address of the MAC address 00:00:f0:aa:bb:cc are extracted and an access vector corresponding to the MAC destination address and an access vector corresponding to the MAC source address are determined. Then the access vector corresponding to the MAC source address is compared to the access vector corresponding to the MAC destination address.

Clearly the present invention is not disclosed by Holloway. "There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention."

Accordingly, the rejection of claim 1 is deemed to be in error and should be withdrawn.

With respect to claim 2, Holloway discloses an anti-hacker table. This table is known as the Authorized Address List (AAL). The Examiner refers to both of Holloway's AAL table and a "Breach list table", and refers to Holloway's disclosure in col. 17, lines 15-17 with respect to an IP address. "In order to provide security protection at the network layer, it will be clear to one skilled in the art that the authorized address list (AAL) described herein can be extended to include IP

addresses."

Accordingly, Holloway's AAL may comprise a port number, a source MAC address and a source IP address. The AAL does not comprise *information pertaining to a plurality of client nodes, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol)* address. Additionally Holloway's AAL does not comprise a plurality of server nodes of a network, wherein *each server node is identified by a corresponding host identification.*

Holloway's Breach list table, Fig. 7, includes a source MAC address that was detected as an intruder, the module and port number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list.. The Breach List contains information on intrusions recognized by the hub and in the process of being secured.

Accordingly, the Breach list table does not comprise *information pertaining to a plurality of client nodes, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol)* address. Additionally Holloway's Breach list table does not comprise a plurality of server nodes of a network, wherein *each server node is identified by a corresponding host identification.*

Further, with respect to the step of *determining whether the received MAC source address is stored in said address table* set forth in claim 2, the Examiner refers us to Holloway's step 132

Step 132 in Holloway's Fig. 11, as noted previously, is directed towards discovering what

devices are connected to a managed hub in order to create an Interconnect Device List (ICD) which identifies those devices authorized to be connected to the hub.

The Interconnect Device List (ICD) is not part of Holloway's AAL (deemed by the Examiner to be the *access table* set forth in claim 1). Therefore, the feature of *determining whether the received MAC source address is stored in said address table* is not met by Holloway's step 132.

Second, Holloway does not disclose *storing the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table.* That is, Holloway does not compare the source MAC address in the AAL table based upon a determination of whether or not the source MAC address is stored in an anti-hacker table.

The Examiner refers us to step 265 in Holloway's Fig. 12. In this step, an entry is added to the Breach List containing the following: MAC address that was detected as the intruder, the module and port number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list.

The Breach list is not part of Holloway's AAL (deemed by the Examiner to be the *access table* set forth in claim 1). Therefore, the feature of *storing the configured address entry for said received MAC source address* ***in said address table*** is not met by Holloway's step 265.

Accordingly, the rejection of claim 2 is deemed to be in error and should be withdrawn.

Claim 3 calls for *modifying an access vector included in said configured address entry for said new MAC source address, to set security; and*

storing the configured address entry including the modified access vector for said new MAC source address in said address table

The Examiner refers to step 320 of Fig. 13, and steps 320 and 322, respectively.

In step 320, a filter is set for the intruding MAC address on the current port. Processing then continues at step 322. In step 322, a check is made to determine if the filter processing has been applied to all of the ports in the interconnect device.

There is no discussion of access vectors nor in changing any part of Holloway's AAL (deemed by the Examiner to be the *access table* set forth in claim 1).

Accordingly, the rejection of claim 3 is deemed to be in error and should be withdrawn.

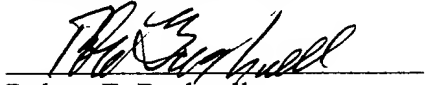
Claims 4-21 are newly added and are deemed to be allowable over the art of record for the same reasons as described above for claims 1-3. And in particular, the prior art fails to disclose or teach an address table, having stored therein, registered MAC addresses, source access vectors corresponding to source MAC addresses of the registered MAC addresses and destination access vectors corresponding to destination MAC addresses of the registered MAC addresses, such that communication is denied, when the source access vectors corresponding to a received MAC address are compared to the destination access vectors corresponding to the received MAC address, the comparison indicates there is no match.

The examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

A fee of $250.00 for one extra dependent claim and one extra independent claim is incurred by filing this Statement.

Should a Petition for extension of time be required with the filing of this Amendment, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if**, a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,



Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56339
Date: 3/9/05
I.D.: REB/MDP